Application No. 09/585,747
Filed: June 2, 2000
TC Art Unit: 2132
Confirmation No.: 7128

REMARKS

In response to an Office Action mailed on June 14, 2004, Applicant respectfully requests that the above-listed Amendments be entered and the Application be reconsidered. With entry of the above-listed Amendments, claims 1, 4-8 are amended; claims 9-11 are canceled; claims 2 and 3 are original; and claims 12-24 are new. Thus, 21 claims are presented for examination. Of these, claims 1, 4, 5 and 8 are independent, and the remaining claims are dependent.

The Examiner rejected claims 1-4 under 35 U.S.C. 103(a) as being obvious over US Pat. No. 6,584,505 to Howard, *et al.* ("Howard") in view of U.S. Pat. No. 6,158,010 to Marconi, *et al.* ("Marconi"). Howard discloses an authentication server that receives login information from a user, authenticates the user and notifies a network server that the user is authenticated, without revealing the login information or other authentication information to the network server. (Howard: Abstract.) Moriconi discloses a policy manager located on a server for managing and distributing a security policy and an application guard located on a client for managing access to securable components as specified by the security policy. (Marconi: Abstract.)

In one aspect, the invention includes a first data processing agent that receives a service request from a user and a second data processing agent that, responsive to a request from the first data processing agent, authenticates the user. If the second data processing agent successfully authenticates the user, the second data processing agent sends authentication information, such as a user name and a password, to the first data processing agent. The first data processing agent stores this authentication information and uses it to authenticate subsequent user requests, without submitting subsequent authentication requests to the second data processing agent. Thus, the first data processing agent maintains a local copy of the authentication information.

In contrast, neither Howard nor Marconi distributes authentication information that would enable an agent to authenticate a user. Howard stores a "cookie" on the user's computer or otherwise notifies the network server that the user has been authenticated. Thus, in response to a subsequent user request, the network server can ascertain that the user has been authenticated. However, Howard clearly states that the user's "login information and the authentication information is concealed from the network server." (Howard: Abstract; emphasis added.)

WEINGARTEN, SCHURGIN
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

Claims 1 and 4 have been amended to recite, "if the user is successfully authenticated, the response includes authentication information that the first data processing agent can use to authenticate a subsequent user service request without submitting a subsequent authentication request to the second data processing agent." No art of record, either alone or in combination, discloses, teaches or suggests a method or system for authenticating a user that provides a response that includes such authentication information to an agent. For at least this reason, claims 1 and 4 are believed to be allowable.

Claims 2, 3 and 12-15 depend directly or indirectly from either claim 1 or claim 4 and are, therefore, believed to be allowable, for at least the reasons discussed above with respect to claims 1 and 4.

The Examiner rejected claims 5-6 and 8-11 under 35 U.S.C. 103(a) as being anticipated by Howard in view of Marconi and U.S. Pat. No. 6,463,474 to Fuh, *et al.* ("Fuh").

Fuh discloses a network device configured to intercept network traffic initiated from a client and directed toward a network resource and locally authenticate the client. If the client is successfully authenticated, the network device is "reconfigured" to allow network traffic initiated by the client to reach the network resource. Thus, a client may be authenticated locally at a router or similar device. (Fuh: Abstract.)

Howard discloses maintaining a maximum amount of time since the user logged in and entered authentication information or "refreshed" the authentication information by re-entering the password. If the user makes an access request to an affiliate server after the maximum time has expired, the user is re-authenticated, i.e. the user must re-enter the password. (Howard: col. 6, lines 1-16.)

According to the claimed invention, the second data processing agent maintains a first timeout period. If the first timeout period expires before a second service request is received from the user, the user is required to be authenticated again by the second data processing agent. Any of a plurality of first data processing agents can receive the service requests from the user. However, unlike the cited art, when a first data processing agent receives a service request from the user, the first timeout period is restarted. Thus, as long as the user makes a service request on any of the first data processing agents before the first timeout period expires, the timeout period is restarted.

WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

Furthermore, as long as the user makes service requests more frequently than the length of the first timeout period, the user is not required to be authenticated again.

Claim 5 has been amended to recite, "if the second service request is received from the user at another of the plurality of first data processing agents before the first time period is exceeded, restarting the first timeout period." Claim 8 has been similarly amended.

In contrast, Howard simply maintains a maximum amount of time since the most recent user login or refresh, regardless of whether the user has remained idle or made service requests since logging in or refreshing the authentication information.

Fuh discloses an "authentication cache inactivity timer," however Fuh's system resides in a router or a similar device that is interposed between a client and a server. For example, Fuh's router can be connected between the client and the Internet, and the server can be accessed via the Internet. Thus, all requests from the client pass through Fuh's router on their way, via the Internet, to the server. Fuh's system must process all requests from the client in order to maintain the inactivity timer.

In contrast, the second data processing agent of the present invention need not process any of the requests from the user. Instead, if any of the plurality of first data processing agents receives a service request from the user, the receiving first data processing agent notifies the second data processing agent of the service request, and the second data processing agent resets the timeout period.

A system according to the present invention operates differently than, and provides advantages over, Fuh's system. For example, if a request is lost on its way from Fuh's router to the server (which frequently happens to requests carried over the Internet), Fuh's system nevertheless treats the request as traffic generated by the client, which prevents an idle timeout event from occurring. In contrast, the first timeout period of the present invention accurately reflects the amount of time left before an actual service request must be received by one of the plurality of first data processing agents before the user is required to be authenticated again. Thus, Fuh's system is reactive to time periods between requests that are sent by the client, whereas systems according to the present invention are reactive to time periods between requests that are actually received by the first data processing agents.

WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX (617) 451-0313

Furthermore, combining Fuh's inactivity timer with the teachings of Howard would not yield the claimed invention. Adding Fuh's inactivity timer to Howard's authentication server would not produce a system that resets a timeout period after the receipt of a user request, because user requests do not flow through Howard's authentication server. Howard's authentication server is invoked only when the user must be authenticated. To reset the timeout period after user requests, each of Howard's affiliated servers would have to be modified to notify the authentication server when the affiliated server receives a user request, as recited in amended claim 5. No art of record discloses, teaches or suggests such a modification.

It is believed a system for authenticating a user that restarts a timeout period after a service request has been received from the user is novel and nonobvious. For at least this reason, claims 5 and 8 are believed to be allowable.

Claims 6, 7 and 12-20 depend directly or indirectly from either claim 5 or claim 8 and are, therefore, believed to be allowable, for at least the reasons discussed above with respect to claims 5 and 8.

The Examiner rejected claim 11 under 35 U.S.C. 103(a) as being compatible over Howard in view of Marconi and Fuh and further in view of U.S. Pat. No. 6,490,624 to Sampson, *et al.* ("Sampson"). Sampson discloses a session management system that maintains a "last access time" as part of its timeout processing. For each session, Sampson employs a session manager 420A or 420B. Each time a runtime 406A or 406B contacts one of the session managers with respect to a particular session, the session manager updates the last access time value associated with the session information for the session. The session manager then notifies all other active session managers and provides the updated time value. (Sampson: col. 14, lines 5-24.)

In contrast, according to the claimed invention, if a first data processing agent receives a service request from the user, the first data processing agent transmits a message to the second data processing agent, and the second data processing agent restarts the first timeout period. The first data processing agent does not need to notify all the other first data processing agents of the service request. This provides an advantage over Sampson, because the claimed invention generates many fewer messages than Sampson's system generates. In particular, the number of messages sent in Sampson's system increases as session managers are added to the system. In contrast, the claimed

WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

invention needs to send only one message, regardless of the number of first data processing agents in the system. Thus, it is not believed that addition of the Sampson reference to the other cited art renders claim 7 obvious.

Claims 9-11 are canceled without prejudice.

For all the foregoing reasons, it is respectfully submitted that the present Application is in a condition for allowance, and such action is earnestly solicited. The Examiner is encouraged to telephone the undersigned attorney to discuss any matter that would expedite allowance of the present Application.

Respectfully submitted,

SMARAGDA HADKINIKITAS, *ET AL.*

By: _____
George J. Jakobsche
Registration No. 39,236
Attorney for Applicant(s)

WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
Ten Post Office Square
Boston, MA 02109
Telephone: (617) 542-2290
Telecopier: (617) 451-0313

GJJ/ad
307730-1

WEINGARTEN, SCHURGIN
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313